(19)日本国特許庁（ＪＰ）　　(12) **公開特許公報**（Ａ）　　(11)特許出願公開番号

特開2000－196616

（P2000－196616A）

(43)公開日　平成12年7月14日(2000.7.14)

(51)Int.Cl.^{7}	識別記号	ＦＩ	テーマコード'(参考)
Ｈ０４Ｌ　12/28		Ｈ０４Ｌ　11/20　　Ｄ	５Ｊ１０４
9/08		Ｈ０４Ｑ　3/00	５Ｋ０３０
9/12		Ｈ０４Ｌ　9/00　　６０１Ｂ	９Ａ００１
12/22		６３１	
Ｈ０４Ｑ　3/00		11/26	

審査請求　未請求　請求項の数21　ＯＬ　（全 17 頁）

(21)出願番号　特願平10－372206

(22)出願日　平成10年12月28日(1998.12.28)

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　小林　浩
東京都港区芝浦一丁目１番１号　株式会社東芝本社事務所内

(72)発明者　大和　克己
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(74)代理人　100083161
弁理士　外川　英明

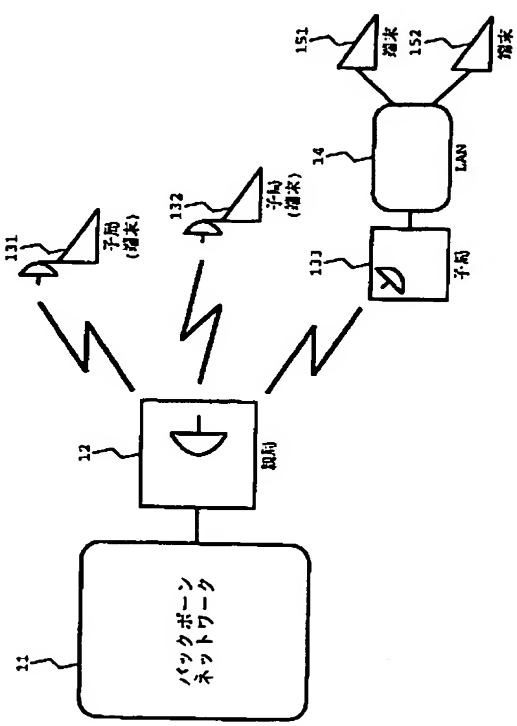
最終頁に続く

(54)【発明の名称】　情報通信ネットワークを用いた暗号化方式

(57)【要約】　　　　（修正有）

【課題】ユーザが意識してアプリケーション層におけるセキュリティ機能を起動させせなくとも、悪意を持つユーザが攻撃から通信データを守る。

【解決手段】複数の子局１３１～１３３と、複数の子局と伝送媒体を用いてＡＴＭセルの送受信を行う親局１２と、子局の一つと親局との組に対して与えられる、ＡＴＭセルの送信時、もしくは受信時に行う暗号化処理、復号処理に用いるセル暗号化鍵と、子局と親局との間での、セル暗号化鍵の更新に伴う同期を取るために、ＡＴＭセルの送信側よりＡＴＭのセルの受信側に対して、暗号化に用いたセル暗号化鍵の更新事項もしくは更新した暗号鍵を使用した事項を通知するセル暗号化鍵更新通知手段とを具備する。



１

【特許請求の範囲】

【請求項１】　バックボーンネットワークに接続する親局と複数の子局とを接続するアクセス回線に相当する共用の伝送媒体を備えた情報通信ネットワークにおいて、前記複数の子局と、前記複数の子局と前記伝送媒体を用いてＡＴＭセルの送受信を行う親局と、前記子局の一つと前記親局との組に対して与えられる、ＡＴＭセルの送信時もしくは受信時に行う暗号化処理及び復号処理に用いるセル暗号化鍵と、前記子局と前記親局との間での、前記セル暗号化鍵の更新に伴う同期を取るために、ＡＴＭセルの送信側よりＡＴＭのセルの受信側に対して、暗号化に用いたセル暗号化鍵の更新事項もしくは更新した暗号鍵を使用した事項を通知するセル暗号化鍵更新通知手段とを具備したことを特徴とする情報通信ネットワークを用いた暗号化方式。

【請求項２】　前記セル暗号化鍵更新通知手段は、ＡＴＭセルの送信側において、セル暗号化鍵の更新後の、ＡＴＭセルヘッダ内の特定の少なくとも１ビットを、セル暗号化鍵の更新前に対して変更することにより通知することを特徴とする、請求項１記載の情報通信ネットワークを用いた暗号化方式。

【請求項３】　前記ＡＴＭセルヘッダ内の特定の少なくとも１ビットは、ＧＦＣフィールド内に割り当てられることを特徴とする請求項２記載の情報通信ネットワークを用いた暗号化方式。

【請求項４】　前記セル暗号化鍵更新通知手段は、ＡＴＭセルの送信側において、セル暗号化鍵の更新事項もしくは更新したセル暗号化鍵を使用した事項を示すＯＡＭセルを生成し送信することにより通知することを特徴とする、請求項１記載の情報通信ネットワークを用いた暗号化方式。

【請求項５】　前記子局の一つと前記親局との組に対して与えられる、セル暗号化鍵の送信時もしくは受信時に行う暗号化処理及び復号処理に用いる鍵暗号化鍵と、前記子局と前記親局との間での、前記鍵暗号化鍵の更新に伴う同期を取るために、セル暗号化鍵の送信側よりセル暗号化鍵の受信側に対して、暗号化に用いた鍵暗号化鍵の更新事項もしくは更新した鍵暗号鍵を使用した事項を通知する鍵暗号化鍵更新通知手段とを具備したことを特徴とする情報通信ネットワークを用いた暗号化方式。

【請求項６】　前記セル暗号化鍵更新通知手段、および前記鍵暗号化鍵更新通知手段は、ＡＴＭセルの送信側において、セル暗号化鍵もしくは鍵暗号化鍵の更新後の、ＡＴＭセルヘッダ内の特定の少なくとも１ビットを、セル暗号化鍵もしくは鍵暗号化鍵の更新前に対して変更することにより通知することを特徴とする請求項５記載の情報通信ネットワークを用いた暗号化方式。

【請求項７】　前記ＡＴＭセルヘッダ内の特定の少なくとも１ビットは、ＧＦＣフィールド内に割り当てられることを特徴とする請求項６記載の情報通信ネットワークを用いた暗号化方式。

２

【請求項８】　前記セル暗号化鍵更新通知手段および前記鍵暗号化鍵更新通知手段は、ＡＴＭセルの送信側において、セル暗号化鍵の更新事項あるいは鍵暗号化鍵の更新事項もしくは更新したセル暗号化鍵あるいは鍵暗号化鍵の使用事項を示すＯＡＭセルを生成し送信することにより通知することを特徴とする請求項５記載の情報通信ネットワークを用いた暗号化方式。

【請求項９】　ネットワーク内の２ノード局間での通信を提供するポイントツーポイント型ネットワークにおいて、第一のノード局と、前記第一のノード局との間でＡＴＭセルの送受信を行う第二のノード局と、前記第一のノード局と前記第二のノード局の組に対して与えられる、ＡＴＭセル送信時もしくは受信時に行う暗号化処理および復号処理に用いるセル暗号化鍵と、前記第一のノード局と前記第二のノード局との間において、前記セル暗号化鍵の更新に伴ない同期を取るにあたって、ＡＴＭセルの送信側よりＡＴＭセルの受信側に対して、暗号化に用いたセル暗号化鍵の更新を行った事項もしくは更新した事項を通知するセル暗号化鍵更新通知手段とを具備したことを特徴とする情報通信ネットワークを用いた暗号化方式。

【請求項１０】　前記セル暗号化鍵更新通知手段は、ＡＴＭセルの送信側において、セル暗号化鍵の更新後の、ＡＴＭセルヘッダ内の特定の少なくとも１ビットを、セル暗号化鍵の更新前に対して変更することにより通知することを特徴とする請求項９記載の情報通信ネットワークを用いた暗号化方式。

【請求項１１】　前記ＡＴＭセルヘッダ内の特定の少なくとも１ビットは、ＶＰＩが記載されるフィールドの内に割り当てられ、前記第一のノード局と前記第二のノード局では、ＶＰＩを規定のＶＰＩフィールド長より短いフィールド長にて表すことを特徴とする請求項１０記載の情報通信ネットワークを用いた暗号化方式。

【請求項１２】　前記ＡＴＭセルヘッダ内の特定の少なくとも１ビットは、ＶＣＩが記載されるフィールドの内に割り当てられ、前記第一のノード局と前記第二のノード局では、前記ＶＣＩを規定のＶＣＩフィールド長より短いフィールド長にて表すことを特徴とする請求項１０記載の情報通信ネットワークを用いた暗号化方式。

【請求項１３】　前記セル暗号化鍵更新通知手段は、ＡＴＭセルの送信側において、セル暗号化鍵を更新した事項もしくは更新したセル暗号化鍵を使用した事項を示すＯＡＭセルを生成し送信することにより通知することを特徴とする請求項９記載の情報通信ネットワークを用いた暗号化方式。

【請求項１４】　前記第一のノード局と前記第二のノード局の組に対して与えられる、セル暗号化鍵の送信時もしくは受信時に行う暗号化処理、復号処理に用いる鍵暗号化鍵と、前記第一のノード局と前記第二のノード局と

の間での、前記鍵暗号化鍵の更新に伴う同期を取るために、セル暗号化鍵の送信側よりセル暗号化鍵の受信側に対して、暗号化に用いた鍵暗号化鍵の更新を行った事項もしくは更新した鍵暗号鍵を使用した事項を通知する鍵暗号化鍵更新通知手段とを具備したことを特徴とする情報通信ネットワークを用いた暗号化方式。

【請求項１５】　前記セル暗号化鍵更新通知手段、および前記鍵暗号化鍵更新通知手段は、ＡＴＭセルの送信側において、セル暗号化鍵もしくは鍵暗号化鍵の更新後の、ＡＴＭセルヘッダ内の特定の少なくとも１ビットを、セル暗号化鍵もしくは鍵暗号化鍵の更新前に対して変更することにより通知することを特徴とする請求項１４記載の情報通信ネットワークを用いた暗号化方式。

【請求項１６】　前記ＡＴＭセルヘッダ内の特定の少なくとも１ビットは、ＶＰＩが記載されるフィールドの内に割り当てられ、前記第一のノード局と前記第二のノード局では、ＶＰＩを規定のＶＰＩフィールド長より短いフィールド長にて表すことを特徴とする請求項１５記載の情報通信ネットワークを用いた暗号化方式。

【請求項１７】　前記ＡＴＭセルヘッダ内の特定の少なくとも１ビットは、ＶＣＩが記載されるフィールドの内に割り当てられ、前記第一のノード局と前記第二のノード局では、ＶＣＩを規定のＶＣＩフィールド長より短いフィールド長にて表すことを特徴とする請求項１５記載の情報通信ネットワークを用いた暗号化方式。

【請求項１８】　前記セル暗号化鍵更新通知手段および前記鍵暗号化鍵更新通知手段は、ＡＴＭセルの送信側において、セル暗号化鍵あるいは鍵暗号化鍵を更新した事項もしくは更新したセル暗号化鍵あるいは鍵暗号鍵を使用した事項を示すＯＡＭセルを生成し送信することにより通知することを特徴とする、請求項１４記載の情報通信ネットワークを用いた暗号化方式。

【請求項１９】　ＡＴＭセルを用いて通信を行うＡＴＭネットワークにおいて、ＡＴＭセルの送信時に、前記ＡＴＭセルのヘッダを圧縮するセルヘッダ圧縮手段と、前記セル圧縮手段により圧縮された前記ＡＴＭセルのヘッダ内の空き領域に、前記ＡＴＭセルに関わる制御情報を記載する制御情報記載手段と、ＡＴＭセルの受信時に前記制御情報記載手段により記載された前記ＡＴＭセルのヘッダ内の前記制御情報を除去する制御情報除去手段と、前記制御情報除去手段により除去された前記ＡＴＭセルのヘッダを規定の形に戻るように伸張するセルヘッダ伸張手段とを具備したことを特徴とするＡＴＭネットワーク。

【請求項２０】　前記セルヘッダ圧縮手段は、　ＶＰＩを規定のＶＰＩフィールド長より短いフィールド長にて表すことを特徴とし、また前記制御情報記載手段は、前記セルヘッダ圧縮手段により空き領域が生じたＶＰＩが記載されるフィールドの内に前記制御情報を記載することを特徴とする請求項１９記載の情報通信ネットワークを用いた暗号化方式。

【請求項２１】　前記セルヘッダ圧縮手段は、　ＶＣＩを規定のＶＣＩフィールド長より短いフィールド長にて表すことを特徴とし、また前記制御情報記載手段は、前記セルヘッダ圧縮手段により空き領域が生じたＶＣＩが記載されるフィールドの内に前記制御情報を記載することを特徴とする請求項１９記載の情報通信ネットワークを用いた暗号化方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、例えば加入者無線アクセスシステムのように、交換やルーティングを司ったり、複数の子局に対するアクセス制御などを行う親局と、加入者装置などの子局とを接続するアクセス回線に相当する伝送媒体を、多数の子局にて共用し合うような、シェアードメディア型アクセスネットワークや、特定の２ノード局間の通信を提供するポイントツーポイント型ネットワーク、そして（「ＡＴＭセル」という。）を用いて通信を行うＡＴＭネットワーク等の情報通信ネットワークを用いた暗号化方式に関する。

【０００２】

【従来の技術】加入者無線アクセスシステム、（以下ＦＴＴＨ(Fiber To The Home)という。）、(以下ＨＦＣ(Hybrid Fiber and Coaxial)という。）等のように、交換やルーティングを司ったり、子局に対するアクセス制御などを行う親局と、加入者装置などの子局とを接続するアクセス回線に相当する伝送媒体を多数の子局にて共用し合う、シェアードメディア型アクセスネットワークが、出現している。その中でも、アクセス回線を無線回線を用いて実現する加入者無線アクセスシステムは、アクセス回線を光ファイバやメタルケーブルを用いて実現しようとする場合アクセス回線の設置、取り換え及び保守を行う際に伴う、道路掘り起こし作業や電信柱に登っての作業が必要であった。他方、上述したシェアードメディア型アクセスネットワークでは、伝送媒体を多数の子局にて共有する、ポイントツーマルチポイント通信（以下「ＰＴＭＰ通信」という。）を提供するため、従来の電話網のように、交換局と加入者装置との間の伝送路をポイントツーポイント通信（以下「ＰＴＰ通信」という。）にて提供する場合に比べて、セキュリティ上の脆弱さが問題となる。例えば、子局を改造することで、他の子局宛への通信データの盗聴が可能となる。そのため、シェアードメディア型アクセスネットワークでは、セキュリティ機能の強化が特に必要となる。
なお、無線ローカルループ（以下「ＷＬＬ」という。）ネットワークのようにネットワーク事業者内のノード局間を無線回線にてポイントツーポイント通信を行うネットワークにおいても、伝送媒体に無線回線を使用しているという特徴上、セキュリティ機能の強化が同様に必要となる。

【０００３】セキュリティ機能を強化するため、アプリケーション層においては、送信相手以外にメッセージ内容を読まれないように、送信メッセージに暗号化処理を施す機能、電子マネー等の情報をやりとりする場合に、偽造されたものではないことを確認できるよう、外部認証局が発行するディジタル署名によって差出人の身元を確認する機能等を搭載することが考えられる。

【０００４】

【発明が解決しようとする課題】前出のように、アプリケーション層において暗号化処理機能やディジタル署名による身元確認機能を搭載することでセキュリティを強化する方法では、ユーザが意識してセキュリティ機能を起動することが前提となるため、ユーザにおいて機密情報を暗号化せずに送信してしまった場合には、通信データに対するセキュリティの保証が全くなされない。本発明の目的は上記の問題点に鑑み、親局と子局との間での伝送媒体（シェアードメディア）を介したＰＴＭＰ通信を提供する上でのセキュリティ機能、さらには特定の２ノード局間のＰＴＰ通信を提供する上でのセキュリティ機能を、アプリケーション層にて施すエンドツーエンドのセキュリティ機能とは別に、ＡＴＭセルの転送を行うＡＴＭ層においても提供するような、シェアードメディア型アクセスネットワーク、そしてポイントツーポイント型ネットワークを提供することにある。ところで、ＡＴＭ層でのセキュリティ機能を提供するために、ＡＴＭセルのペイロード情報に対して暗号化処理を施す場合、さらなるセキュリティ強化のために、当該暗号化に用いる暗号化鍵を更新することが考えられる。その際に、ＡＴＭセルの送信側と受信側との間にて、暗号化鍵の更新の同期を取るために、ＡＴＭセルの送信側よりＡＴＭのセルの受信側に対して、暗号化に用いた暗号化鍵の更新を行った旨の情報、もしくは更新した暗号鍵を使用している旨の情報を通知する必要がある。しかしながら、ＡＴＭ通信の標準化団体にて規定されたＡＴＭセルヘッダ内には、前記情報を記載するための領域が存在しない。

【０００５】本発明の目的は上記の問題点も鑑み、暗号化鍵の更新の同期を取るために必要な情報をはじめとする、ＡＴＭ通信の標準化団体にて規定されていない、ＡＴＭセルに関わる制御情報を記載するための領域を、ＡＴＭセルヘッダ内に確保することを可能とする、ＡＴＭネットワークを提供することにある。

【０００６】

【課題を解決するための手段】上記目的を解決するために第一の発明は、親局と子局とを接続するアクセス回線に相当する伝送媒体を多数の子局にて共用し合うシェアードメディア型アクセスネットワークにおいて、複数の子局と、前記複数の子局と前記伝送媒体を用いてＡＴＭセルの送受信を行う親局と、前記子局の一つと前記親局との組に対して与えられる、ＡＴＭセルの送信時、もしくは受信時に行う暗号化処理、復号処理に用いるセル暗号化鍵と、前記子局と前記親局との間での、前記セル暗号化鍵の更新に伴う同期を取るために、ＡＴＭセルの送信側よりＡＴＭのセルの受信側に対して、暗号化に用いたセル暗号化鍵の更新を行った旨、もしくは更新した暗号鍵を使用している旨を通知するセル暗号化鍵更新通知手段と、を具備したことを特徴とする。なお、前記セル暗号化鍵更新通知手段は、ＡＴＭセルの送信側において、セル暗号化鍵の更新後の、ＡＴＭセルヘッダ内の特定の少なくとも１ビットを、セル暗号化鍵の更新前に対して変更することにより通知することを特徴とする。前記ＡＴＭセルヘッダ内の特定の少なくとも１ビットは、ＧＦＣフィールド内に割り当てられることを特徴とする。

【０００７】また、前記セル暗号化鍵更新通知手段は、ＡＴＭセルの送信側において、セル暗号化鍵を更新した旨、もしくは更新したセル暗号化鍵を使用している旨を示すＯＡＭセルを生成し送信することにより通知することを特徴とする。このように構成することにより、親局と子局との間でのシェアードメディアを介したＰＴＭＰ通信を提供する上でのセキュリティ機能を、アプリケーション層にて施すエンドツーエンドのセキュリティ機能とは別に、ＡＴＭ層において、ＡＴＭセルに対して暗号化処理を施して当該ＡＴＭセルを送信するというセキュリティ機能を新たに提供することができ、ユーザが意識してアプリケーション層におけるセキュリティ機能を起動させなくとも、悪意を持つユーザの攻撃から通信データを守ることが可能となる。さらに、ＡＴＭセルの送信時の暗号化処理、復号処理の際に用いるセル暗号化鍵の更新に伴う、親局と子局との間で使用する鍵の更新の同期を、ＧＦＣフィールド値、もしくはＯＡＭセルを用いて陽に取ることで、送信側にて暗号化処理に使用する共通鍵を定期的に更新する場合でも、受信側において正しい共通鍵を用いた復号処理を正確に行うことができる。

【０００８】一方、第二の発明は、親局と子局とを接続するアクセス回線に相当する伝送媒体を多数の子局にて共用し合うシェアードメディア型アクセスネットワークにおいて、複数の子局と、前記複数の子局と前記伝送媒体を用いてＡＴＭセルの送受信を行う親局と、前記子局の一つと前記親局との組に対して与えられる、ＡＴＭセルの送信時、もしくは受信時に行う暗号化処理、復号処理に用いるセル暗号化鍵と、前記子局と前記親局との間での、前記セル暗号化鍵の更新に伴う同期を取るために、ＡＴＭセルの送信側よりＡＴＭのセルの受信側に対して、暗号化に用いたセル暗号化鍵の更新を行った旨、もしくは更新した暗号鍵を使用している旨を通知するセル暗号化鍵更新通知手段と、前記子局の一つと前記親局との組に対して与えられる、セル暗号化鍵の送信時、もしくは受信時に行う暗号化処理、復号処理に用いる鍵暗号化鍵と、前記子局と前記親局との間での、前記鍵暗号化鍵の更新に伴う同期を取るために、セル暗号化鍵の送

信側よりセル暗号化鍵の受信側に対して、暗号化に用いた鍵暗号化鍵の更新を行った旨、もしくは更新した鍵暗号化鍵を使用している旨を通知する鍵暗号化鍵更新通知手段と、を具備したことを特徴とする。

【０００９】なお、前記セル暗号化鍵更新通知手段、および前記鍵暗号化鍵更新通知手段は、ＡＴＭセルの送信側において、セル暗号化鍵もしくは鍵暗号化鍵の更新後の、ＡＴＭセルヘッダ内の特定の少なくとも１ビットを、セル暗号化鍵もしくは鍵暗号化鍵の更新前に対して変更することにより通知することを特徴とする。前記ＡＴＭセルヘッダ内の特定の少なくとも１ビットは、ＧＦＣフィールド内に割り当てられることを特徴とする。また、前記セル暗号化鍵更新通知手段、および前記鍵暗号化鍵更新通知手段は、ＡＴＭセルの送信側において、セル暗号化鍵あるいは鍵暗号化鍵を更新した旨、もしくは更新したセル暗号化鍵あるいは鍵暗号化鍵を使用している旨を示すＯＡＭセルを生成し送信することにより通知することを特徴とする。このように構成することにより、親局と子局との間でのシェアードメディアを介したＰＴＭＰ通信を提供する上でのセキュリティ機能を、ＡＴＭセルの送信に対してだけでなく、ＡＴＭセルの暗号化処理、復号処理に用いるセル暗号化鍵の送信に対しても新たに提供することができる。さらに、親局と子局との間で使用する鍵の更新の同期を、セル暗号化鍵に対してだけでなく、鍵暗号化鍵に対しても、ＧＦＣフィールド値、もしくはＯＡＭセルを用いて陽に取ることで、送信側にて暗号化処理に使用する共通鍵を定期的に更新する場合でも、受信側において正しい共通鍵を用いた復号処理を正確に行うことができる。

【００１０】第三の発明は、ネットワーク内の２ノード局間での通信を提供するポイントツーポイント型ネットワークにおいて、第一のノード局と、前記第一のノード局との間でＡＴＭセルの送受信を行う第二のノード局と、前記第一のノード局と前記第二のノード局の組に対して与えられる、ＡＴＭセルの送信時、もしくは受信時に行う暗号化処理、復号処理に用いるセル暗号化鍵と、前記第一のノード局と前記第二のノード局との間での、前記セル暗号化鍵の更新に伴う同期を取るために、ＡＴＭセルの送信側よりＡＴＭセルの受信側に対して、暗号化に用いたセル暗号化鍵の更新を行った旨、もしくは更新したセル暗号化鍵を使用している旨を通知するセル暗号化鍵更新通知手段と、を具備したことを特徴とする。なお、前記セル暗号化鍵更新通知手段は、ＡＴＭセルの送信側において、セル暗号化鍵の更新後の、ＡＴＭセルヘッダ内の特定の少なくとも１ビットを、セル暗号化鍵の更新前に対して変更することにより通知することを特徴とする。前記ＡＴＭセルヘッダ内の特定の少なくとも１ビットは、ＶＰＩが記載されるフィールドの内に割り当てられ、前記第一のノード局と前記第二のノード局では、ＶＰＩを、規定のＶＰＩフィールド長より短いフィールド長にて表すことを特徴とする。

【００１１】前記ＡＴＭセルヘッダ内の特定の少なくとも１ビットは、ＶＣＩが記載されるフィールドの内に割り当てられ、前記第一のノード局と前記第二のノード局では、ＶＣＩを、規定のＶＣＩフィールド長より短いフィールド長にて表すことを特徴とする。　また、前記セル暗号化鍵更新通知手段は、ＡＴＭセルの送信側において、セル暗号化鍵を更新した旨、もしくは更新したセル暗号化鍵を使用している旨を示すＯＡＭセルを生成し送信することにより通知することを特徴とする。このように構成することにより、シェアードメディアを介したＰＴＭＰ通信だけでなく、ＰＴＰ通信を提供する上でのセキュリティ機能を、アプリケーション層にて施すエンドツーエンドのセキュリティ機能とは別に、ＡＴＭ層において、ＡＴＭセルに対して暗号化処理を施して当該ＡＴＭセルを送信するというセキュリティ機能を新たに提供することができ、ユーザが意識してアプリケーション層におけるセキュリティ機能を起動させなくとも、悪意を持つユーザの攻撃から通信データを守ることが可能となる。さらに、ＡＴＭセルの送信時の暗号化処理、復号処理の際に用いるセル暗号化鍵の更新に伴う、ノード局間で使用する鍵の更新の同期を、ＶＰＩフィールドまたはＶＣＩフィールドを圧縮することにより生じる空きビット領域、もしくはＯＡＭセルを用いて陽に取ることで、送信側にて暗号化処理に使用する共通鍵を定期的に更新する場合でも、受信側において正しい共通鍵を用いた復号処理を正確に行うことができる。

【００１２】一方、第四の発明は、ネットワーク内の２ノード局間での通信を提供するポイントツーポイント型ネットワークにおいて、第一のノード局と、前記第一のノード局との間でＡＴＭセルの送受信を行う第二のノード局と、前記第一のノード局と前記第二のノード局の組に対して与えられる、ＡＴＭセルの送信時、もしくは受信時に行う暗号化処理、復号処理に用いるセル暗号化鍵と、前記第一のノード局と前記第二のノード局との間での、前記セル暗号化鍵の更新に伴う同期を取るために、ＡＴＭセルの送信側よりＡＴＭのセルの受信側に対して、暗号化に用いたセル暗号化鍵の更新を行った旨、もしくは更新したセル暗号化鍵を使用している旨を通知するセル暗号化鍵更新通知手段と、前記第一のノード局と前記第二のノード局の組に対して与えられる、セル暗号化鍵の送信時、もしくは受信時に行う暗号化処理、復号処理に用いる鍵暗号化鍵と、前記第一のノード局と前記第二のノード局との間での、前記鍵暗号化鍵の更新に伴う同期を取るために、セル暗号化鍵の送信側よりセル暗号化鍵の受信側に対して、暗号化に用いた鍵暗号化鍵の更新を行った旨、もしくは更新した鍵暗号化鍵を使用している旨を通知する鍵暗号化鍵更新通知手段と、を具備したことを特徴とする。

【００１３】なお、前記セル暗号化鍵更新通知手段、お

よび前記鍵暗号化鍵更新通知手段は、ＡＴＭセルの送信側において、セル暗号化鍵もしくは鍵暗号化鍵の更新後の、ＡＴＭセルヘッダ内の特定の少なくとも１ビットを、セル暗号化鍵もしくは鍵暗号化鍵の更新前に対して変更することにより通知することを特徴とする。前記ＡＴＭセルヘッダ内の特定の少なくとも１ビットは、ＶＰＩが記載されるフィールドの内に割り当てられ、前記第一のノード局と前記第二のノード局では、ＶＰＩを、規定のＶＰＩフィールド長より短いフィールド長にて表すことを特徴とする。前記ＡＴＭセルヘッダ内の特定の少なくとも１ビットは、ＶＣＩが記載されるフィールドの内に割り当てられ、前記第一のノード局と前記第二のノード局では、ＶＣＩを、規定のＶＣＩフィールド長より短いフィールド長にて表すことを特徴とする。また、前記セル暗号化鍵更新通知手段、および前記鍵暗号化鍵更新通知手段は、ＡＴＭセルの送信側において、セル暗号化鍵あるいは鍵暗号化鍵を更新した旨、もしくは更新したセル暗号化鍵あるいは鍵暗号化鍵を使用している旨を示すＯＡＭセルを生成し送信することにより通知することを特徴とする。

【００１４】このように構成することにより、ＰＴＰ通信を提供する上でのセキュリティ機能を、ＡＴＭセルの送信に対してだけでなく、ＡＴＭセルの暗号化処理、復号処理に用いるセル暗号化鍵の送信に対しても新たに提供することができる。さらに、ノード局間で使用する鍵の更新の同期を、セル暗号化鍵に対してだけでなく、鍵暗号化鍵に対しても、ＶＰＩフィールドまたはＶＣＩフィールドを圧縮することにより生じる空きビット領域、もしくはＯＡＭセルを用いて陽に取ることで、送信側にて暗号化処理に使用する共通鍵を定期的に更新する場合でも、受信側において正しい共通鍵を用いた復号処理を正確に行うことができる。第五の発明は、ＡＴＭセルを用いて通信を行うＡＴＭネットワークにおいて、ＡＴＭセルの送信時に、前記ＡＴＭセルのヘッダを圧縮するセルヘッダ圧縮手段と、前記セル圧縮手段により圧縮された前記ＡＴＭセルのヘッダ内の空き領域に、前記ＡＴＭセルに関わる制御情報を記載する制御情報記載手段と、ＡＴＭセルの受信時に、前記制御情報記載手段により記載された前記ＡＴＭセルのヘッダ内の前記制御情報を除去する制御情報除去手段と、前記制御情報除去手段により除去された前記ＡＴＭセルのヘッダを規定の形に戻るように伸張するセルヘッダ伸張手段と、を具備したことを特徴とする。

【００１５】前記セルヘッダ圧縮手段は、　ＶＰＩを規定のＶＰＩフィールド長より短いフィールド長にて表すことを特徴とし、また、前記制御情報記載手段は、前記セルヘッダ圧縮手段により空き領域が生じた、ＶＰＩが記載されるフィールドの内に前記制御情報を記載することを特徴とする。前記セルヘッダ圧縮手段は、　ＶＣＩを規定のＶＣＩフィールド長より短いフィールド長にて表すことを特徴とし、また、前記制御情報記載手段は、前記セルヘッダ圧縮手段により空き領域が生じた、ＶＣＩが記載されるフィールドの内に前記制御情報を記載することを特徴とする。このように構成することにより、暗号化鍵の更新の同期を取るために必要な情報をはじめとする、ＡＴＭ通信の標準化団体にて規定されていない、ＡＴＭセルに関わる制御情報を記載するための領域を、ＶＰＩフィールド、ＶＣＩフィールドをはじめとするＡＴＭセルヘッダ内に確保することができる。

【００１６】

【発明の実施の形態】図１は、この発明に係わるシェアードメディア型アクセスネットワークの一つである、加入者無線アクセスシステムのアーキテクチャの一実施の形態を示す図である。図１において、１１はバックボーンネットワーク、１２は交換やルーティングを司ったり、子局に対するアクセス制御などを行う親局、１３１～１３３は加入者装置などの子局である。親局１２と子局１３１～１３３は伝送媒体として無線回線が用いられている。また、バックボーンネットワーク１１と親局１２とは、有線回線もしくは無線回線を用いて接続される。そして、子局１３３にはＬＡＮ１４を介して端末１５１、１５２が接続されており、子局１３１、１３２は端末である。図１に示す加入者無線アクセスシステムでは、親局１２と子局１３１～１３３との間の通信を無線回線という同一の伝送媒体を用いて行うため、親局とある子局との間の通信データを、他の子局が盗聴することは、自身の子局を改造することで容易に行うことができる。本発明では、このような他の子局による通信データの盗聴を防ぐためのセキュリティ機能を、従来アプリケーション層にて施されている、エンドツーエンドのセキュリティ機能とは別に提供する。

【００１７】図２は、図１に示した加入者無線アクセスシステムがＡＴＭ（非同期転送モード）を用いて通信を行う場合の、親局１２と端末１５１（もしくは端末１５２）との間のプロトコルスタック（図２の（ａ））、そして親局１２と子局１３１（もしくは子局１３２）との間のプロトコルスタック（図２の（ｂ））を示す。図２において、Applic.はアプリケーション層を、ＡＡＬはＡＴＭアダプテーション層を、ＡＴＭはＡＴＭ層を、ＰＨＹは物理層を示す。また、ＷＡＬは無線アクセス層を示し、無線回線上でＡＴＭ通信を実現するためのプロトコルを規定している。本発明では、他の子局と共有する無線回線を使用した通信が行われる、親局と子局との間でのデータ通信に対してセキュリティ機能を新たに搭載する。そのために、親局、子局のＡＴＭ層に、セキュリティ機能を搭載するものとする（ＡＴＭ＋Ｓｅｃ層）。ＡＴＭ＋Ｓｅｃ層では、通常のＡＴＭ層にて行う動作に加えて、以下の動作を行うことが可能である。（１）受信したＡＴＭセルのペイロード情報を暗号化する。（２）受信したＡＴＭセルのペイロード情報が暗号化さ

れていれば、本情報を復号する。

【００１８】このようにＡＴＭセルを単位に暗号化する場合、ＡＴＭ層の上位層に混在する様々なサービス（ＩＰ（インターネットプロトコル）パケット転送サービス、ＭＡＣ（メディアアクセス制御）パケット転送サービス、音声データサービス、専用線サービス、等）に対するセキュリティ機能の強化を、これらのサービスに依存せずに、ＡＴＭ層にて統一した方法にて提供することが可能となる。図３～図５は、図２に示したＡＴＭ＋Ｓｅｃ層にて行う、暗号化、復号の手順を示す機能ブロック図である。図３の方法では、親局より子局宛への、下り方向のＡＴＭセルの送信を行う場合、親局内の暗号化部２１１において、親局が保持する子局用の公開鍵を用いてＡＴＭセルの暗号化処理を行い、子局内の復号化部２２１において、子局が保持する秘密鍵を用いて暗号化されたＡＴＭセルの復号処理を行う。また逆に、子局より親局宛への、上り方向のＡＴＭセルの送信を行う場合、子局内の暗号化部２２２において、子局が保持する親局用の公開鍵を用いてＡＴＭセルの暗号化処理を行い、親局内の復号化部２１２において、親局が保持する秘密鍵を用いて暗号化されたＡＴＭセルの復号処理を行う。図３の方法の場合、親局内の暗号化部２１１にて用いる公開鍵、復号化部２１２にて用いる秘密鍵、子局内の暗号化部２２２にて用いる公開鍵、復号化部２２１において用いる秘密鍵は、各々異なるものとなる。

【００１９】図４の方法では、親局内の暗号化／復号化部２１、子局内の暗号化／復号化部２２において用いられる鍵は、親局内の鍵ａ生成部２３にて生成される鍵ａである。そして、親局より子局に対して鍵ａを送信する際に、親局内の暗号化部２４において、親局が保持する子局用の公開鍵を用いて鍵ａの暗号化処理を行い、子局内の復号化部２５において、子局が保持する秘密鍵を用いて暗号化された鍵ａの復号処理を行う。なお、鍵ａの送信には、例えばＡＴＭ通信にて規定されるＯＡＭセル(Operation Administration and Maintenanceセル)を用いることが考えられる。図４の方法の場合、鍵ａ生成部において鍵ａの更新を定期的もしくはランダムな時間間隔に行うことで、送信中のＡＴＭセルの盗聴に対するより強固な防御が実現でき、図３の方法に比べて、さらなるセキュリティ機能の強化が実現できる。また一般に、暗号化処理、復号処理を同一な鍵ａを用いて実行する共通鍵方式の方が、暗号化処理に用いる鍵（公開鍵）と復号処理に用いる鍵（秘密鍵）とを別個に用意する公開鍵方式よりも、暗号化／復号の処理速度が速いので、より高速な通信に向いている。

【００２０】図５の方法では、親局内の暗号化／復号化部２１、子局内の暗号化／復号化部２２において用いられる鍵ａを送信する際に、親局内にて暗号化処理を行う暗号化部２４、子局内にて復号処理を行う復号化部２５において用いられる鍵は、親局内の鍵ｂ生成部２６にて生成される鍵ｂである。そして、親局より子局に対して鍵ｂを送信する際に、親局内の暗号化部２７において、親局が保持する子局用の公開鍵を用いて鍵ｂの暗号化処理を行い、子局内の復号化部２８において、子局が保持する秘密鍵を用いて暗号化された鍵ｂの復号処理を行う。なお、鍵ｂの送信には、例えばＡＴＭ通信にて規定されるＯＡＭセルを用いることが考えられる。図５の方法の場合、鍵ａ生成部における鍵ａの更新を定期的もしくはランダムな時間間隔に行うと共に、鍵ｂ生成部において鍵ｂの更新を定期的もしくはランダムな時間間隔に行うことで、親局より子局宛に送信される鍵ａの盗聴に対するより強固な防御が実現でき、図４の方法に比べて、さらなるセキュリティ機能の強化が実現できる。例えば、鍵ａの更新は半日程度毎に、鍵ｂの更新は一週間程度毎に更新する。なお、公開鍵、秘密鍵を用いた暗号化処理、復号処理（図３におけるＡＴＭセルの暗号化処理、復号処理、図４における鍵ａの暗号化処理、復号処理、図５における鍵ｂの暗号化処理、復号処理）には、例えばＲＳＡ方式(Rivest ShamirAdleman方式)や楕円暗号方式などの公開鍵方式を用いて行い、鍵ａ、鍵ｂを用いた暗号化処理、復号処理（図４、５におけるＡＴＭセルの暗号化処理、復号処理、図５における鍵ａの暗号化処理、復号処理）には、例えばＤＥＳ方式(DataEncryption Standard方式）やＦＥＡＬ方式(Fast Encryption Algorithm方式）などの共通鍵方式を用いて行う。現在のコンピュータ処理能力から、公開鍵方式では７６８ビット以上のビット長の鍵を、共通鍵方式では６４ビット以上のビット長の鍵を用いるのが適当である。

【００２１】本明細書では、セキュリティ機能が一番強固であると考えられる図５の方法を用いた場合の、本発明の実施の形態を、以降において説明する。図６、図７に、図５に示した機能ブロック図にて用いられる共通鍵ａ、ｂの更新の手順を示す。通常、暗号鍵は有効期限を有しており、同期限内に暗号鍵を更新しなければ無効となってしまうため、以降の送信データの復号が不可能となってしまう。図６に示した手順では、暗号鍵を生成する親局が、当該鍵の有効期限前の一定期間に入ると新たな鍵を生成して、子局宛に送信を行う。なお、子局の立ち上げ時に限り、子局より親局宛へ当該子局が立ち上がった旨を通知し、親局にて当該子局の認証を行い、その後に暗号鍵の生成、送信を行う。図７に示した手順では、子局が、暗号鍵の有効期限前の一定期間に入ると、新たな鍵を生成するよう親局宛に共通鍵の生成要求を送信する。なお、子局の立ち上げの際には、子局より親局宛へ当該子局が立ち上がった旨を通知すると共に暗号鍵の生成要求を送信し、親局にて当該子局の認証を行った後に、暗号鍵の生成、送信が行われるようにする。図６および図７に示した手順に従い、親局と子局とにおいて暗号鍵の更新を行う場合、更新前の暗号鍵と更新後の暗号鍵とのいずれの鍵により暗号化処理、復号処理を行う

かを確認する、換言すれば親局と子局との間にて鍵更新の同期を取る必要がある。本発明では、暗号鍵の更新の同期を、（1）ＡＴＭセルヘッダ内の情報（ＧＦＣフィールドなど）を用いる方法（2）ＯＡＭセルを用いる方法のいずれかの方法にて実現する。

【００２２】まず、ＡＴＭセルヘッダ内の情報を用いて暗号鍵の更新の同期を取る方法について説明する。図８に、親局と子局との間で伝送されるＡＴＭセルのフォーマットを示す。図１に示す加入者無線アクセスシステムでは、キャリアが提供するバックボーン網側の設備である親局と、ユーザ側の設備である子局とのインタフェースは、ＵＮＩ（ユーザ網インタフェース）が用いられるので、図８に示したＡＴＭセルのフォーマットは、ＵＮＩにて定義されるものである。図８に示すように、ＡＴＭセルは、情報伝送に必要な情報を格納する５バイト長のヘッダ３１と、伝達情報を格納する４８バイト長のペイロード３２から構成される。ヘッダ３１内には、４ビット長のＧＦＣ(Generic Flow Control)フィールド３３が存在する。ＩＴＵ－Ｔの規格においては、ＧＦＣフィールドは、通信網と端末との間でローカルに行われるフロー制御のために設けたフィールドであるが、通常はＧＦＣフィールドを用いたフロー制御を必要としない。そこで、本発明では、ＧＦＣフィールドのうち１ビットを、暗号鍵の更新の同期を取るために使用する。図９、図１０に、ＧＦＣフィールドの１ビットを用いた暗号鍵の同期の手順を示す。なお、図９では、共通鍵の生成を行う親局より子局宛にＡＴＭセルを送信する場合を、図１０では、子局より親局宛にＡＴＭセルを送信する場合を示す。

【００２３】図９、図１０共に、送信側では、ＡＴＭセルの暗号化に用いた暗号鍵を更新する度に、当該ＡＴＭセル内のＧＦＣフィールドのあらかじめ定められた１ビット（図９、図１０では、ＧＦＣフィールドの下位１ビット）を反転させて送信する。そして受信側では、受信したＡＴＭセルのＧＦＣフィールドの前記１ビットが、前回受信したＡＴＭセルの１ビットと反転した値であれば、予め生成した、もしくは予め受信した、更新後の暗号鍵を用いて暗号化されたＡＴＭセルであることが分かるため、以後、ＧＦＣフィールドの前記１ビットが反転したＡＴＭセルを新たに受信するまでは、当該暗号鍵を用いて復号処理を行う。本方式により、受信側においては、送信側が暗号化処理に用いた暗号鍵が更新前の鍵であるか更新後の鍵であるかを陽に理解することができるため、暗号鍵の定期的あるいはランダムな時間周期で更新を伴う場合にも、復号処理を正確に行うことができる。また、暗号鍵の更新の同期を、未使用領域であるＡＴＭセルヘッダ領域内（ＧＦＣフィールド）の１ビットのみを用いて実現するため、スループットの低下をもたらすことはない。なお、ＡＴＭセルの暗号化を行う加入者無線アクセスシステム以外のネットワークノード（ＡＴＭ交換機、もしくは端末）において、ＧＦＣフィールド内の値に基づくフロー制御機能が搭載されている場合、上述したように暗号鍵の更新の同期を行うために設定したＧＦＣフィールド値を前記ノードにそのまま引き渡すと、予期せぬ動作を引き起こしかねない。そのため、本発明を実施する場合には、暗号鍵による復号処理を終えた受信側では、ＧＦＣフィールドの値４ビットを全て「０」と設定するという手順を行うように規定し、加入者無線アクセスシステム以外のネットワークノードにおいても、ＧＦＣフィールドを用いたフロー制御は行われないようにするという手順を行ってもよい。また、暗号鍵の更新の同期を取るために、前述のようにＧＦＣフィールド内の特定の１ビットを割り当てる他にも、ＶＰＩ値、ＶＣＩ値のいずれか、もしくは両値を圧縮して運用することで、ＶＰＩフィールド（８ビット長）もしくはＶＣＩフィールド（１６ビット長）のいずれか、もしくは両フィールドのうちの一部フィールドに空きビット領域を用意し、本領域を暗号鍵の更新の同期を取るために用いる方法が考えられる。なお、本方法については、別途説明する。

【００２４】次に、ＯＡＭセルを用いて暗号鍵の更新の同期を取る方法について説明する。図１１、図１２に、ＯＡＭセルを用いた暗号鍵の同期の手順を示す。なお、図１１では、共通鍵の生成を行う親局より子局宛にＡＴＭセルを送信する場合を、図１２では、子局より親局宛にＡＴＭセルを送信する場合を示す。図１１、図１２共に、送信側では、ＡＴＭセルの暗号化に用いた暗号鍵を更新する度に、以後のＡＴＭセルに対しては新たな暗号鍵を用いて暗号化を行う旨を示すＯＡＭセルを送信する。そして受信側では、ＯＡＭセルを受信することで、以後に到着するＡＴＭセルが、予め生成した、もしくは予め受信した、更新後の暗号鍵を用いて暗号化されたものであることが分かるため、以後、ＯＡＭセルを新たに受信するまでは、当該暗号鍵を用いて復号処理を行う。なお、図１１に示すように、共通鍵の生成を行う親局がデータの送信側となる場合には、暗号鍵を送信するために用いるＯＡＭセルのみを送信するだけで、受信側である子局においては、以後の親局から送信されるＡＴＭセルは、当該ＯＡＭ内に挿入されている、更新後の暗号鍵を用いて暗号化されるものと認識するようにし、上記ＯＡＭセルとは別に、更新後の暗号鍵を用いて暗号化を開始した旨を示すＯＡＭセルを送信する必要はない。ところで、暗号鍵を更新した旨をＯＡＭセルにて通知する場合、廃棄等により受信側にて当該ＯＡＭセルが正しく受信できなければ、受信側では暗号鍵が更新された旨を知ることができず、以降に受信するＡＴＭセルの復号も更新前の暗号鍵を用いて試みるため、ＡＴＭセルの復号が正しく行われない。これを解決するため、例えば、受信側においては、暗号鍵を更新した旨を示すＯＡＭセルを受信すれば、ＡＣＫを示すセル（ＯＡＭセルを用いて定

義）を折り返し送信側に送信し、送信側においては、当該ＡＣＫを示すセルの受信を待って、新たな暗号鍵に更新するという手段を用いることが考えられる。この場合、送信側では、暗号鍵を更新した旨を示すＯＡＭセルを送信した後も、当該ＯＡＭセルに対するＡＣＫを示すセルを受信するまでは、引き続いて更新前の暗号鍵を用いてＡＴＭセルの暗号化を行い、また、一定時間が経過してもＡＣＫを示すセルが受信できなければ、送信側は再度暗号鍵を更新した旨を示すＯＡＭセルを送信する。

【００２５】他の方法としては、ＡＣＫを示すセルを用いて鍵の更新通知の確認を待つことなく、ＡＴＭセルを更新後の暗号鍵を用いて暗号化して送信し、受信側では正しく復号できたか否かを、例えばパリティチェック機能を用いて認識するという手段も考えられる。この場合、正しく復号できなかったと判断した受信側では、その旨を送信側へ通知し、送信側において、再度暗号鍵を更新した旨を示すＯＡＭセルの送信を行う。図１３は、子局の電源投入時（立ち上げ時）に行われる、親局での当該子局の認証シーケンスを示す。子局では、電源投入時に、子局の認証要求として、公開鍵と子局の識別番号を親局に対して送信する。なお、子局には、当該子局の識別番号、公開鍵、秘密鍵が、予め（子局の製造時、出荷時、等に）記載されている。親局では、送られてきた子局の識別番号が登録されてるものと一致すれば、鍵暗号化鍵（図５における鍵ｂ）を生成し、これを当該子局より送られてきた公開鍵を使って暗号化し、子局に返送する。子局では、子局内に格納している秘密鍵を使ってこれを復号し、鍵暗号化鍵を取得する。次に子局は、鍵暗号化鍵を使って、子局を利用するユーザが入力したパスワード（もしくはこれに代替し得るもの）を暗号化し、親局に送付する。親局では、同じ鍵暗号化鍵を使って復号し、登録されているパスワードと一致すれば正しい子局と認定し、認証手続きを終了する。

【００２６】図１４は、子局の機能ブロック図の一例である。ＡＴＭセル受信部４０１は、子局がＬＡＮもしくは端末と接続する場合は（図１に示す子局１３３）、接続されるノードより発せられるＡＴＭセルを受信し、子局が端末である場合は（図１に示す子局１３１、１３２）、子局の上位層にて生成されるＡＴＭセルを受信する。ＡＴＭセル受信部４０１にて受信したＡＴＭセルは、ＶＰＩ／ＶＣＩ識別部４０２に転送され、当該ＡＴＭセルが属するフロー（ＶＰＩ／ＶＣＩにて一意に識別可能）に基づき、当該ＡＴＭセルの暗号化を行うか否かを判断する。暗号化を行わないフローである場合は、ＡＴＭセル送信部４０３を介して、親局宛に当該セルは送信され、暗号化を行うフローである場合は、当該セルをセル暗号化処理部４０４へ引き渡し、当該セルのペイロード部の暗号化を行う。セル暗号化処理部４０４に引き渡されたＡＴＭセルは、セル暗号化鍵記憶部４０５にて記憶されるセル暗号化鍵（図５に示す鍵ａ）を用いて暗号化が行われた後に、ＡＴＭセル送信部４０３を介して、親局宛に送信される。このとき、ＧＦＣフィールドを用いて親局とのセル暗号化鍵の更新の同期を取る場合は、ＧＦＣビット設定部４０６により、セル暗号化鍵の更新が行われた際に、所定のビットの反転が行われるよう、ＧＦＣビット値の設定が行われる。また、ＯＡＭセルを用いて親局とのセル暗号化鍵の更新の同期を取る場合は、セル暗号化鍵の更新が行われた際に、鍵の更新を行った旨を示すＯＡＭセルをＯＡＭセル生成部４０７にて生成し、親局宛に送信する。なお、セル暗号化鍵の有効期限に伴う新たなセル暗号化鍵の生成要求を親局宛に行う場合は、その旨を示すＯＡＭセルをＯＡＭセル生成部４０７にて生成し、親局宛に送信する。

【００２７】親局より送信されるＡＴＭセルを受信するＡＴＭセル受信部４０８では、受信したＡＴＭセルがＯＡＭセルでなければ、当該セルをＶＰＩ／ＶＣＩ識別部４０９に転送して、当該ＡＴＭセルが属するフローに基づき、当該ＡＴＭセルが暗号化されたＡＴＭセルであるか否かを判断する。暗号化されていないＡＴＭセルである場合は、ＡＴＭセル送信部４１０を介して、当該子局に接続されるノード宛、もしくは当該子局の上位層へＡＴＭセルを送信する。そして当該ＡＴＭセルが暗号化されたＡＴＭセルである場合は、当該セルをセル復号処理部４１１へ引き渡し、当該セルのペイロード部の復号を行う。セル復号処理部４１１に引き渡されたＡＴＭセルは、セル暗号化鍵記憶部４０５にて記憶されているセル暗号化鍵を用いて復号が行われた後に、ＡＴＭセル送信部４１０を介して、送信される。このとき、セル暗号化鍵更新検査部４１２において、セル復号処理部４１１に引き渡されたＡＴＭセル内のＧＦＣビット値のチェック、もしくは、ＯＡＭセル処理部４１３にてセル暗号化鍵の更新を行った旨のＯＡＭセルを受信したか否かのチェックを行い、セル復号処理部４１１にて使用するセル暗号化鍵を更新するか否かを、セル暗号化鍵記憶部４０５へ通知する。

【００２８】ＯＡＭセル処理部４１３では、セル暗号化鍵の更新を行った旨を示すＯＡＭセルの他に、セル暗号化鍵を含むＯＡＭセル、そしてセル暗号化鍵の暗号化処理、復号処理に用いる鍵暗号化鍵（図５に示す鍵ｂ）を含むＯＡＭセルを受信する。暗号化されたセル暗号化鍵を含むＯＡＭセルを受信した場合は、当該鍵をセル暗号化鍵復号処理部４１４へ引き渡し、鍵暗号化鍵記憶部４１５内の鍵暗号化鍵を用いて、セル暗号化鍵を復号し、セル暗号化鍵記憶部４０５へ引き渡す。また、暗号化された鍵暗号化鍵を含むＯＡＭセルを受信した場合は、当該鍵を鍵暗号化鍵復号処理部４１６へ引き渡し、秘密鍵記憶部４１７内の秘密鍵を用いて、鍵暗号化鍵を復号し、鍵暗号化鍵記憶部４１５へ引き渡す。なお、鍵暗号化鍵の有効期限に伴う新たな鍵暗号化鍵の生成要求を親局宛に行う場合は、その旨を示すＯＡＭセルをＯＡＭセ

ル生成部４０７にて生成し、親局宛に送信する。図１５は、親局の機能ブロック図の一例である。子局より送信されるＡＴＭセルを受信するＡＴＭセル受信部５０１では、受信したＡＴＭセルがＯＡＭセルでなければ、当該セルをＶＰＩ／ＶＣＩ識別部５０２に転送して、当該ＡＴＭセルが属するフロー（ＶＰＩ／ＶＣＩにて一意に識別可能）に基づき、当該ＡＴＭセルが暗号化されたＡＴＭセルであるか否かを判断する。暗号化されていないＡＴＭセルである場合は、ＡＴＭセル送信部５０３を介して、当該親局が接続するバックボーン網宛へＡＴＭセルを送信する。そして当該ＡＴＭセルが暗号化されたＡＴＭセルである場合は、当該セルをセル復号処理部５０４へ引き渡し、当該セルのペイロード部の復号を行う。

【００２９】セル復号処理部５０４に引き渡されたＡＴＭセルは、セル暗号化鍵記憶部５０５にて記憶されるセル暗号化鍵（図５に示す鍵ａ）を用いて復号が行われた後に、ＡＴＭセル送信部５０３を介して、送信される。このとき、セル暗号化鍵更新検査部５０６において、セル復号処理部５０４に引き渡されたＡＴＭセル内のＧＦＣビット値のチェック、もしくは、ＯＡＭセル処理部５０７にてセル暗号化鍵の更新を行った旨のＯＡＭセルを受信したか否かのチェックを行い、セル復号処理部５０４にて使用するセル暗号化鍵を更新するか否かを、セル暗号化鍵記憶部５０５へ通知する。バックボーン網より送信されるＡＴＭセルを受信するＡＴＭセル受信部５０８にて受信したＡＴＭセルは、ＶＰＩ／ＶＣＩ識別部５０９に転送され、当該ＡＴＭセルが属するフローに基づき、当該ＡＴＭセルの暗号化を行うか否かを判断する。暗号化を行わないフローである場合は、ＡＴＭセル送信部５１０を介して、子局宛に当該セルは送信され、暗号化を行うフローである場合は、当該セルをセル暗号化処理部５１１へ引き渡し、当該セルのペイロード部の暗号化を行う。セル暗号化処理部５１１に引き渡されたＡＴＭセルは、セル暗号化鍵記憶部５０５にて記憶されるセル暗号化鍵を用いて暗号化が行われた後に、ＡＴＭセル送信部５１０を介して、子局宛に送信される。このとき、ＧＦＣフィールドを用いて子局とのセル暗号化鍵の更新の同期を取る場合は、ＧＦＣビット設定部５１２により、セル暗号化鍵の更新が行われた際に、指定したビットの反転が行われるよう、ＧＦＣビット値の設定が行われる。また、ＯＡＭセルを用いて子局とのセル暗号化鍵の更新の同期を取る場合は、セル暗号化鍵の更新が行われた際に、鍵の更新を行った旨を示すＯＡＭセルをＯＡＭセル生成部５１３にて生成し、子局宛に送信する。

【００３０】セル暗号化鍵生成部５１４では、セル暗号化鍵の有効期限に伴う新たなセル暗号化鍵の生成を、セル暗号化鍵記憶部５０５からの要求、もしくは子局からの要求（ＯＡＭセル処理部５０７にて認識した後に通知）により行う。セル暗号化鍵生成部にて生成されたセル暗号化鍵は、セル暗号化鍵記憶部５０５に引き渡すと共に、セル暗号化鍵暗号化処理部５１５にて暗号化を行った後に、ＯＡＭセル生成部５１３にて当該鍵を挿入したＯＡＭセルを生成し、これを子局宛に送信する。セル暗号化鍵暗号化処理部５１５では、鍵暗号化鍵記憶部５１６内に保持される鍵暗号化鍵（図５に示す鍵ｂ）を用いて、セル暗号化鍵の暗号化を行う。鍵暗号化鍵生成部５１７では、鍵暗号化鍵の有効期限に伴う新たな鍵暗号化鍵の生成を、鍵暗号化鍵記憶部５１６からの要求、もしくは子局からの要求（ＯＡＭセル処理部５０７にて認識した後に通知）により行う。鍵暗号化鍵生成部にて生成された鍵暗号化鍵は、鍵暗号化鍵記憶部５１６に引き渡すと共に、鍵暗号化鍵暗号化処理部５１８にて暗号化を行った後に、ＯＡＭセル生成部５１３にて当該鍵を挿入したＯＡＭセルを生成し、これを子局宛に送信する。鍵暗号化鍵暗号化処理部５１８では、公開鍵記憶部５１９内に保持される公開鍵を用いて、鍵暗号化鍵の暗号化を行う。

【００３１】以上、本発明の実施の形態を加入者無線アクセスシステムを用いて説明したが、これらの発明の実施の形態は、加入者無線アクセスシステムに限らず、親局と複数の加入者との間にて行う通信を同一の伝送媒体を用いて行う、シェアードメディア型アクセスネットワーク全てに適用できるものである。また，上記説明では、親局にてセル暗号鍵及び鍵暗号鍵を生成するとしているが、どちらか一方もとしくは両者の機能を子局が具備しても同様のセキュリティ機能を発揮することができる。なお鍵暗号鍵を子局で生成する場合には，生成した鍵暗号鍵を親局に伝送する際には、子局毎あるいはすべての子局に共通な公開鍵を親局から通知を受けた公開鍵を使って暗号化すればよい。図１６は、この発明に係わるポイントツーポイント型ネットワークのアーキテクチャの一実施の形態を示す図である。図１６において、６１１～６１６はノード局であり、これらはループ状に構成され、そして、ノード局間の通信には無線もしくは有線回線が用いられる。当然ながら、本発明の実施されるネットワークのノード局の構成はループ状に限定されるものではなく、メッシュ状の構成等、他の様々な構成にも適用可能である。また、各々のノード局には、加入者網６２１～６２６が、有線回線もしくは無線回線を用いて接続される。

【００３２】各々のノード局は、隣接するノード局から送信されるデータを受信して、当該データが本ノード局と接続する加入者網宛のデータであればこれを加入者網宛に送出し、そうでなければ他方に隣接するノード局宛に当該データを送出する。また、本ノード局と接続する加入者網より送信されるデータを、隣接するいずれか一方のノード局宛に送出する。図１７は、図１６に示した、無線回線を介して構成されるポイントツーポイント型ネットワークがＡＴＭを用いて通信を行う場合の、ノード局間のプロトコルスタックを示す。ポイントツーポ

イント型ネットワークにおいても、第三者によるデータの盗聴を防ぐために、ノード局のＡＴＭ層に、セキュリティ機能を搭載する（ＡＴＭ＋Ｓｅｃ層）。ＡＴＭ＋Ｓｅｃ層にて行う、暗号化、復号の手順は、図３～図５に示す手順と同様に行うことができる。ＡＴＭセルの配送時に行う暗号化処理、復号処理の際に用いる共通鍵ａ、鍵ａの配送時に行う暗号化処理、復号処理の際に用いる共通鍵ｂ、鍵ｂの配送時に行う暗号化処理、復号処理の際に用いる公開鍵、秘密鍵を用いた場合の機能ブロック図を、図１８に示す。ノード局間にて暗号化処理、復号処理を伴うＡＴＭセルの送受信を行う場合、まず、いずれのノード局にて鍵ａ、鍵ｂを生成するかを取り決める必要がある。図１８の場合、ノード局ａにおいて、これらの共通鍵の生成を行い、ノード局ｂとのＡＴＭセルの送受信を行っている。共通鍵の生成を行うノード局の定め方としては、例えば、ネットワーク構築時に共通鍵を生成するノード局を陽に定めておき、当該ノード局に対してのみ、共通鍵を生成し、送信する機能を搭載させる方法、また、全てのノード局内に共通鍵を生成し、送信する機能を搭載させ、ＡＴＭサービスの開始時に、いずれのノード局にて共通鍵を生成するかを、シグナリング等を用いて規定する方法、等が考えられる。

【００３３】そして、ノード局ａ内の暗号化／復号化部２１、ノード局ｂ内の暗号化／復号化部２２において用いられる鍵ａは、ノード局ａ内の鍵ａ生成部２３にて定期的に生成し、ノード局ｂ宛に送信される。また、鍵ａを送信する際に、ノード局ａ内にて暗号化処理を行う暗号化部２４、ノード局ｂ内にて復号処理を行う復号化部２５において用いられる鍵ｂは、ノード局ａ内の鍵ｂ生成部２６にて定期的に生成し、ノード局ｂ宛に送信される。この時、ノード局ａ内の暗号化部２７にて鍵ｂの暗号化に用いる鍵は公開鍵であり、ノード局ｂ内の復号化部２８にて鍵ｂの復号に用いる鍵は秘密鍵である。ノード局ａとノード局ｂとにおいて、暗号鍵の更新を行う場合、更新前の暗号鍵と更新後の暗号鍵とのいずれの鍵により暗号化処理、復号処理を行うかを、親局と子局との間にて同期を取る必要がある。そのための一つの方法として、前出した加入者無線アクセスシステムにおいて示した、ＯＡＭセルを用いて行う方法を挙げることができる。その際の手順は、図１１、図１２と同様に行われる。ところで、前出した加入者無線アクセスシステムにおいて示した、暗号鍵の更新の同期を取る方法の一つである、ＧＦＣフィールドを用いる方法は、図１６に示すノード局間にてＡＴＭセルの送受信を行う場合には適用できない。これは、本ノード局間のインタフェースとしては、ＵＮＩではなくＮＮＩ（ネットワークノードインタフェース）が用いられるためである。図１９に、ノード局間で伝送される、ＮＮＩにて定義されるＡＴＭセルのフォーマットを示すが、ＮＮＩにて定義されるＡＴＭセルでは、ヘッダ３１内にＧＦＣフィールドが存在しないことが原因である。

【００３４】そこで本発明では、ＮＮＩにて定義されるＡＴＭセルのヘッダ内の情報を用いて暗号鍵の更新の同期を取るため、ＶＰＩフィールド（１２ビット長）もしくはＶＣＩフィールド（１６ビット長）のいずれか、もしくは両フィールドのうちの一部フィールドを、暗号鍵の更新の同期を取るために用いる方法を示す。そのためには、ＶＰＩ値、ＶＣＩ値のいずれか、もしくは両値を圧縮して運用する必要がある。図２０に、ＶＰＩ値圧縮の手順を示す。図２０の例では、ＶＰＩ値のみを圧縮して、ＶＣＩ値については圧縮を行わない方法を示すが、当然ながら、ＶＣＩ値のみを圧縮する方法、ＶＰＩ値、ＶＣＩ値の両値を圧縮する方法も、同様の手順にて実現できる。図２０では、あるキャリアが提供するキャリア網７１（例えば、図１６に示すポイントツーポイント型ネットワーク）内において、ローカルなＶＰＩ値「ＶＰＩ－Ｌ」を定義する。ＶＰＩ－Ｌ値は、図２０では１１ビット長としているが、それ以下のビット長であっても良い。そして、キャリア網７１のインタフェース部７２、７３では、外部より受信したＡＴＭセル内のＶＰＩ値をＶＰＩ－Ｌ値に変換してキャリア網内へ送信し、またキャリア網より受信したＡＴＭセル内のＶＰＩ－Ｌ値を当初のＶＰＩ値に変換して外部へ送信する。図２０の場合、インタフェース部７２において、外部からのＡＴＭセルの受信を、インタフェース部７３において、外部へのＡＴＭセルの送信を行っている。

【００３５】１２ビット長にて定義されるＶＰＩ値と、キャリア網７１内でローカルに定義されるＶＰＩ－Ｌ値との対応表７２１、７３１は、インタフェース部７２、７３内にて各々保持される。これらの対応表は、新たな仮想コネクションの設定要求時に、当該仮想コネクションのＶＰＩ値に、本ＶＰＩ値に対応させる、キャリア網７１内にて生成したＶＰＩ－Ｌ値とが、新たなエントリとして挿入され、仮想コネクションの解放時に、当該仮想コネクションのＶＰＩ値と、本ＶＰＩ値に対応するＶＰＩ－Ｌ値とが記載されたエントリが、消去される。図２０に示したＶＰＩ圧縮により、キャリア網７１においてはＶＰＩフィールド内に、１１ビット長のＶＰＩ－Ｌ値が挿入されるため、図２１に示すように、ＶＰＩフィールドの１ビット領域が未使用となる。そこで、この未使用となる１ビット領域（以後、本領域を空きビット領域と呼ぶ）を、暗号鍵の更新の同期を取るために用いる。なお、図２１にて示したＡＴＭセルフォーマットは、キャリア網７１内にてローカルに使用され、キャリア網７１内のノードでは、ＶＰＩフィールドの内の１１ビット領域にてＶＰＩ値（ＶＰＩ－Ｌ値）を認識し、残りの１ビットを、暗号鍵の更新の同期を取るためのビットと認識する。

【００３６】図２０では、キャリア網内でのＶＰＩ値の圧縮（ＶＰＩ－Ｌ値への変換）を、インタフェース部内

に対応表を用意することにより実現する方法を示したが、他にも、例えば、MH(Modified Huffman)符号化方式のような圧縮アルゴリズム、そして当該アルゴリズムにて圧縮されたデータを復号するアルゴリズムをインタフェース部内に搭載することにより、ＶＰＩフィールド内に未使用ビット領域を生成し、これを暗号鍵の更新の同期を取るために用いる方法も考えられる。上記空きビット領域を、暗号鍵の更新の同期を取るために使用する例を、図２２、図２３に示す。なお、図２２では、共通鍵の生成を行うノード局ａよりノード局ｂ宛にＡＴＭセルを送信する場合を、図２３では、ノード局ｂよりノード局ａ宛にＡＴＭセルを送信する場合を示す。図２２、図２３共に、送信側では、ＡＴＭセルの暗号化に用いた暗号鍵を更新する度に、当該ＡＴＭセル内の上記空きビット領域１ビットを反転させて送信する。そして受信側では、受信したＡＴＭセルの当該領域１ビットが、前回受信したＡＴＭセルの１ビットと反転した値であれば、予め生成した、もしくは予め受信した、更新後の暗号鍵を用いて暗号化されたＡＴＭセルであることが分かるため、以後、当該領域の前記１ビットが反転したＡＴＭセルを新たに受信するまでは、当該暗号鍵を用いて復号処理を行う。

【００３７】なお、前述のシェアードメディア形アクセスネットワークでは、ＧＦＣフィールド内の特定の１ビットを鍵更新の同期用に割り当てるとしていたが、本実施例と同様にＶＰＩ／ＶＣＩを圧縮して、空きビット領域を同期用に割り当てても良いことは付言するまでもない。また、本実施の形態では、ＶＰＩ値、もしくはＶＣＩ値を圧縮することにより生じる空きビット領域を、暗号鍵の更新の同期を取るために使用しているが、その他にも、キャリア網内に閉じたローカルな制御を提供するために、本領域を使用することが可能である。ＡＴＭセルのヘッダ内には、当該ＡＴＭセルの損失の優先表示を行うＣＬＰ(Cell Loss Priority)ビットが１ビットのみ用意され、本値を元に、ネットワーク内ではＡＴＭセルの優先制御を行う。しかしながら、ＣＬＰビットにて表示可能な優先レベルは２レベルのみであり（ＣＬＰ＝０、ＣＬＰ＝１；ＣＬＰ＝０の方が優先度が高い）、より細かな優先レベルを表示することは不可能である。そこで、任意のネットワーク内において、よりきめ細かなＡＴＭセルの優先制御をローカルに実行するために、ＶＰＩ値、もしくはＶＣＩ値を圧縮することにより生じる空きビット領域を、ＡＴＭセルの優先度表示に使用しても良い。ＡＴＭセルの優先度を、ＣＬＰビットと当該空きビット領域とを組み合わせて表示することにより、４レベルの優先レベルの表示が可能となり、ＣＬＰビットのみを用いた場合に比べてより細かな優先制御の実現が可能となる。

【００３８】当該空きビット領域は、上述したような暗号鍵の更新の同期情報やセルの優先度といった情報の記載に利用する他にも、例えば、より強固な誤り制御を提供するために、ＡＴＭセル内情報に対するパリティビットの設定に使用する等、様々な制御情報の記載に用いることができる。特に、ＡＴＭ通信の標準化団体で規定されていない制御情報をネットワーク内にてローカルに規定してＡＴＭセル内に記載したい場合に、ＡＴＭセルヘッダの圧縮により当該空きビット領域を生成すれば、これが可能となる。

【００３９】

【発明の効果】以上説明したように、本発明は、親局と子局との間でのシェアードメディアを介したポイントツーマルチポイント通信を提供する上でのセキュリティ機能、そして、ネットワーク内のノード局間でのポイントツーポイント通信を提供する上でのセキュリティ機能を、アプリケーション層にて施すエンドツーエンドのセキュリティ機能とは別に、ＡＴＭ層において、ＡＴＭセルに対して暗号化処理を施して当該ＡＴＭセルを送信するというセキュリティ機能を新たに提供することで、ユーザが意識してアプリケーション層におけるセキュリティ機能を起動させなくとも、悪意を持つユーザの攻撃から通信データを守ることが可能となる。さらに、ＡＴＭセルの送信時の暗号化処理、復号処理の際に用いる共通鍵（セル暗号化鍵）、そしてこの共通鍵の送信時の暗号化処理、復号処理の際に用いる共通鍵（鍵暗号化鍵）の更新に伴う、親局と子局との間で使用する鍵の更新の同期を、ＧＦＣフィールドもしくはＯＡＭセルを用いて陽に取ることで、そしてネットワーク内のノード局間で使用する鍵の更新の同期を、ＶＰＩフィールドまたはＶＣＩフィールドを圧縮することにより生じる空きビット領域、もしくはＯＡＭセルを用いて陽に取ることで、送信側にて暗号化処理に使用する共通鍵を定期的に更新する場合でも、受信側において正しい共通鍵を用いた復号処理を正確に行うことができる。

【００４０】また、ＡＴＭセルヘッダを圧縮して、ＶＰＩフィールド、ＶＣＩフィールドとはじめとするＡＴＭセルヘッダ内に、ＡＴＭ通信の標準化団体で規定されていない、ネットワーク内にてローカルに定義した制御情報を記載するための領域を確保することにより、新たな制御セルを挿入することなく、これらの制御情報の通知が可能となるため、制御セルの挿入に伴うスループットの低下を防いだ上で、より高度なネットワーク制御の実現が可能となる。

【図面の簡単な説明】

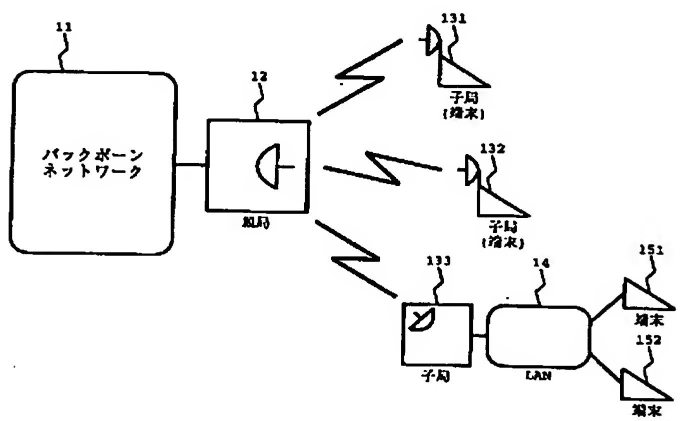
【図１】この発明に係わるシェアードメディア型ネットワークの一つ、加入者無線アクセスシステムのアーキテクチャの一実施の形態を示す図。

【図２】図１に示した加入者無線アクセスシステムがＡＴＭを用いて通信を行う場合のプロトコルスタックを示す図。

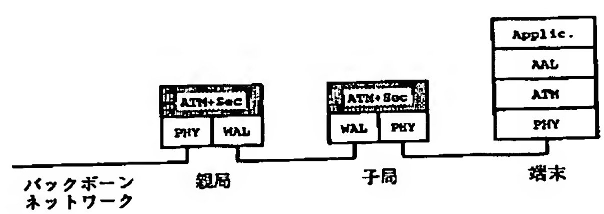
【図３】図１に示した加入者無線アクセスシステムがＡ

ＴＭを用いて通信を行う場合のプロトコルスタックを示す別の対応図。
【図４】図２に示したＡＴＭ＋Ｓｅｃ層にて行う、公開鍵、秘密鍵を用いた暗号化、復号の手順を示す機能ブロック図。
【図５】図２に示したＡＴＭ＋Ｓｅｃ層にて行う、公開鍵、秘密鍵、共通鍵ａを用いた暗号化、復号の手順を示す機能ブロック図。
【図６】図２に示したＡＴＭ＋Ｓｅｃ層にて行う、公開鍵、秘密鍵、共通鍵ａ、ｂを用いた暗号化、復号の手順を示す機能ブロック図。
【図７】共通鍵ａ、ｂの更新の手順の実施の形態を示す図。
【図８】共通鍵ａ、ｂの更新の手順の、図６とは異なる実施の形態を示す図。
【図９】ＵＮＩにて定義されるＡＴＭセルのフォーマットを示す図。
【図１０】親局より子局宛にＡＴＭセルを送信する場合の、ＧＦＣフィールドの１ビットを用いた暗号鍵の同期の手順を示す図。
【図１１】子局より親局宛にＡＴＭセルを送信する場合の、ＧＦＣフィールドの１ビットを用いた暗号鍵の同期の手順を示す図。
【図１２】親局より子局宛にＡＴＭセルを送信する場合の、ＯＡＭセルを用いた暗号鍵の同期の手順を示す図。
【図１３】子局より親局宛にＡＴＭセルを送信する場合の、ＯＡＭセルを用いた暗号鍵の同期の手順を示す図。
【図１４】子局の電源投入時に行われる、親局での子局の認証シーケンスを示す図。
【図１５】子局の機能ブロック図の一例を示す図。
【図１６】親局の機能ブロック図の一例を示す図。
【図１７】この発明に係わるポイントツーポイント型ネットワークのアーキテクチャの一実施の形態を示す図。
【図１８】図１６に示したポイントツーポイント型ネットワークがＡＴＭを用いて通信を行う場合のプロトコルスタックを示す図。
【図１９】図１７に示したＡＴＭ＋Ｓｅｃ層にて行う、公開鍵、秘密鍵、共通鍵ａ、ｂを用いた暗号化、復号の手順を示す機能ブロック図。
【図２０】ＮＮＩにて定義されるＡＴＭセルのフォーマットを示す図。
【図２１】ＶＰＩ値圧縮の手順を示す図。
【図２２】ＶＰＩ値圧縮を行った際の、ＮＮＩにて定義されるＡＴＭセルのフォーマットを示す図。
【図２３】ノード局ａよりノード局ｂ宛にＡＴＭセルを送信する場合の、ＶＰＩ値圧縮後の空きビット領域を用いた暗号鍵の同期の手順を示す図。
【図２４】ノード局ｂよりノード局ａ宛にＡＴＭセルを送信する場合の、ＶＰＩ値圧縮後の空きビット領域を用いた暗号鍵の同期の手順を示す図。
【符号の説明】

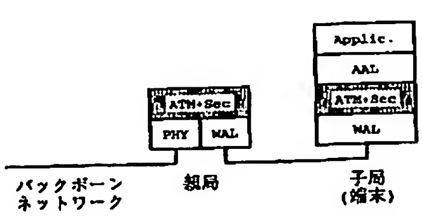
【図１】



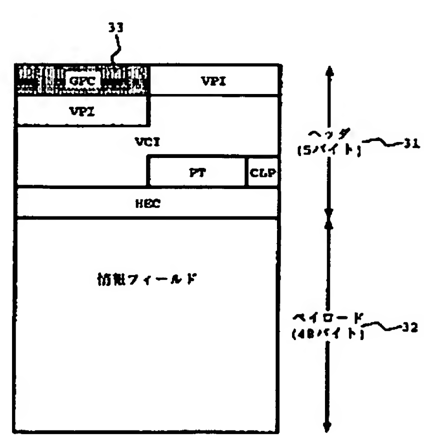
【図２】



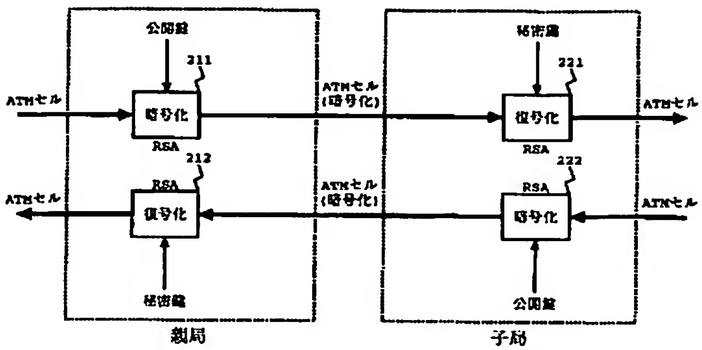
【図３】



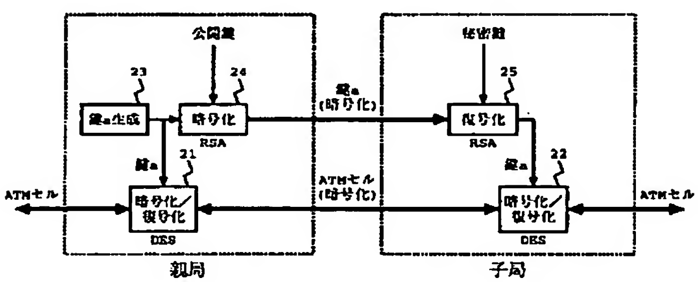
【図９】



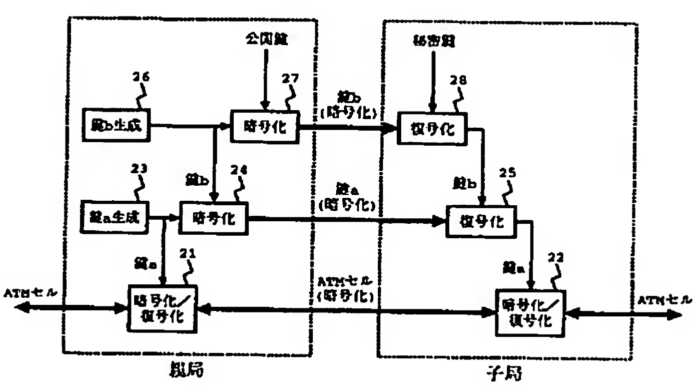
【図４】



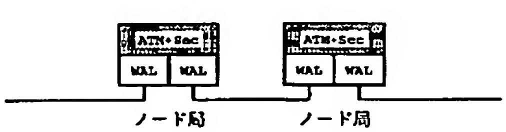
【図５】



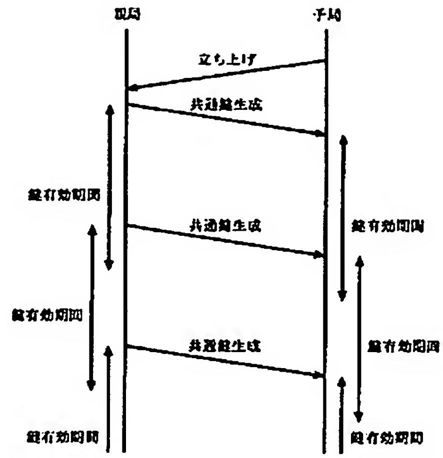
【図６】



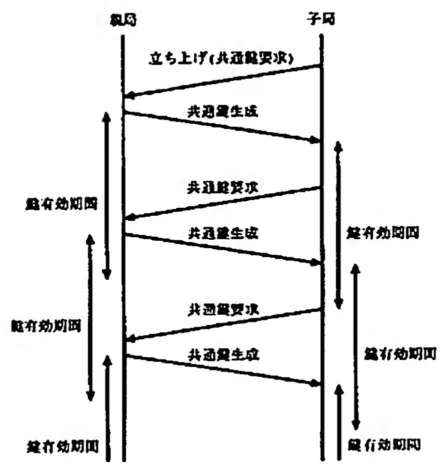
【図１８】



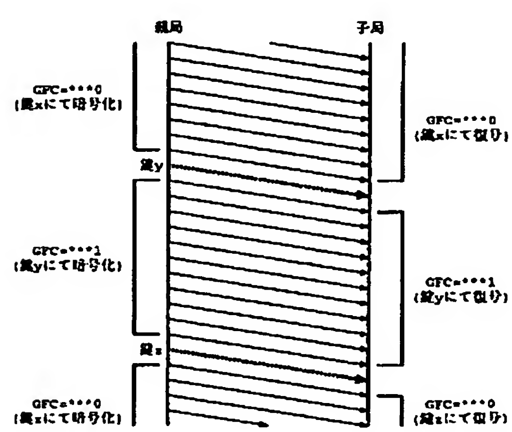
【図７】



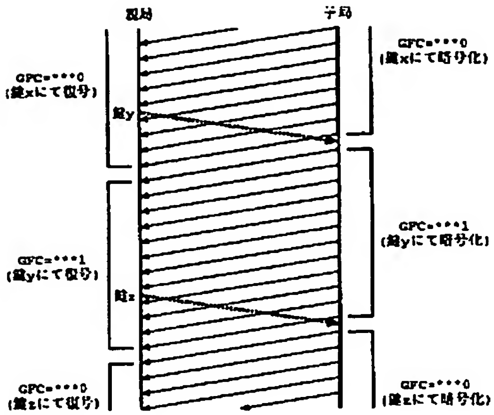
【図８】



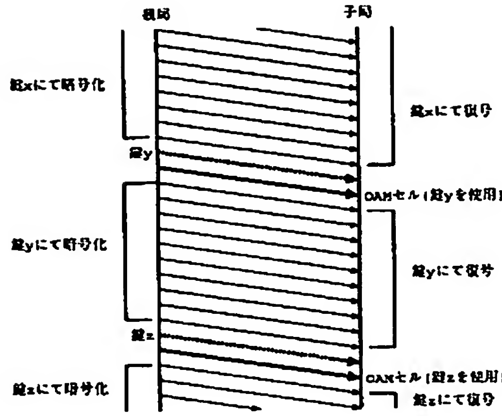
【図１０】



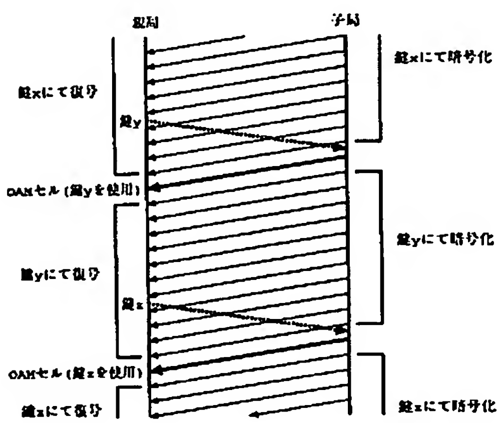
【図１１】



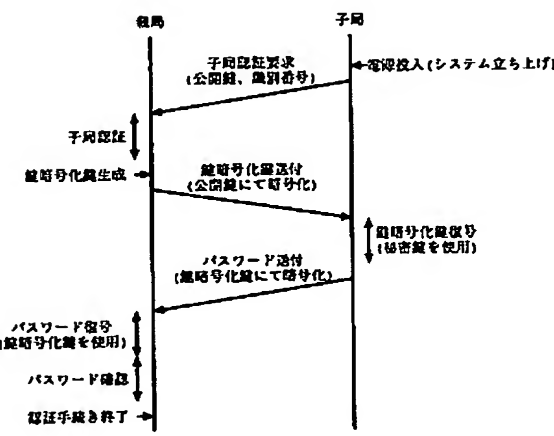
【図１２】



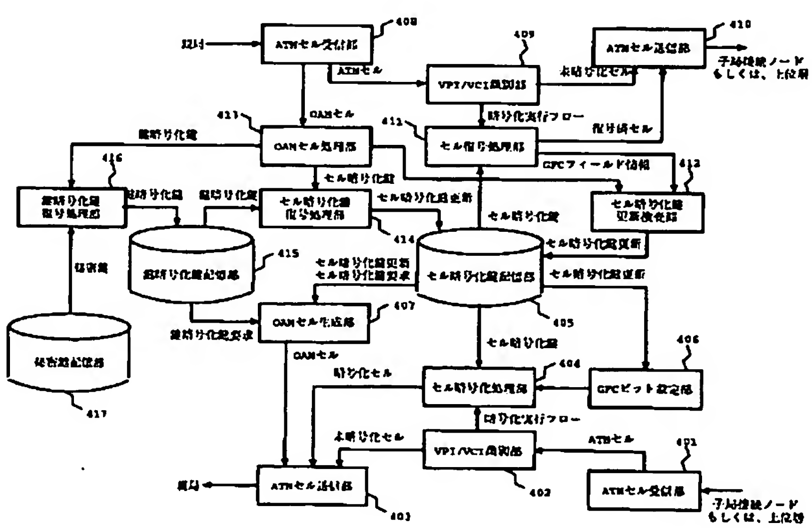
【図１３】



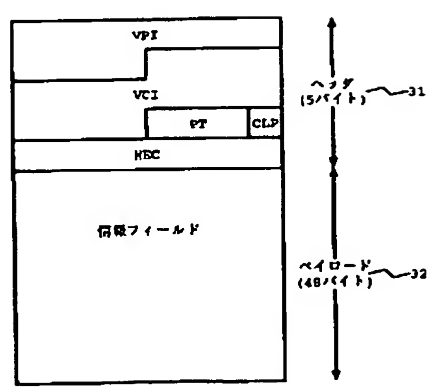
【図１４】



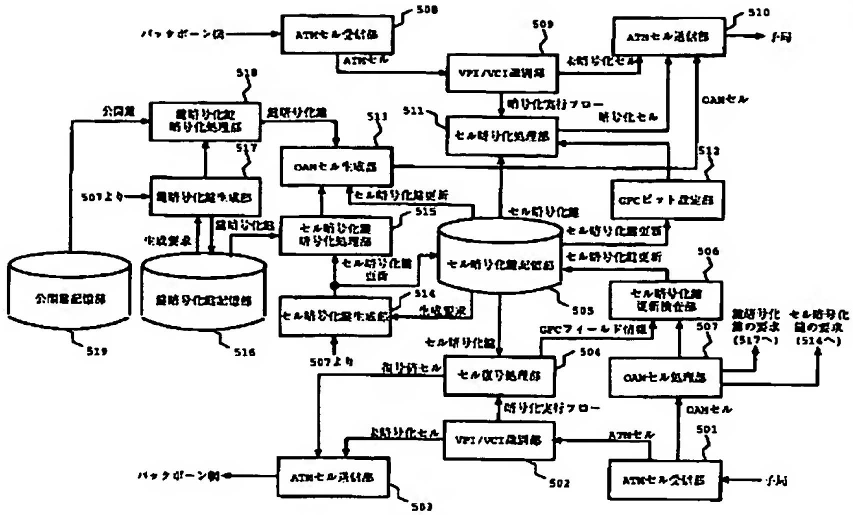
【図１５】



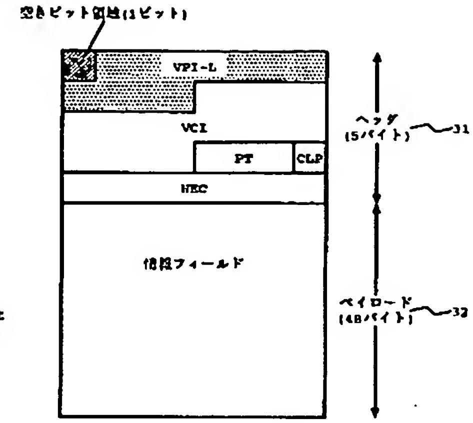
【図２０】



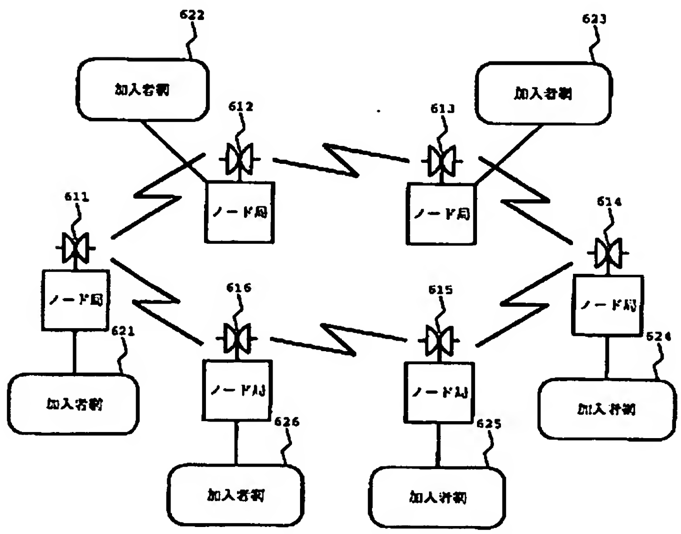
【図１６】



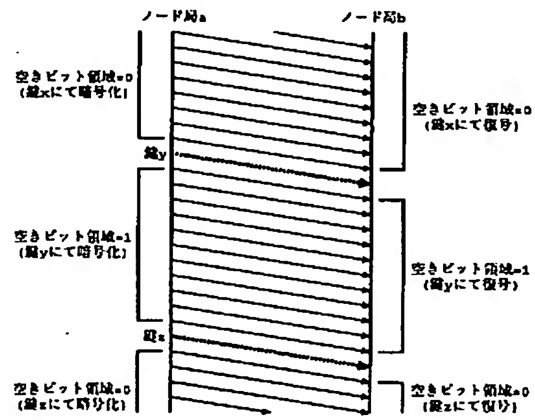
【図２２】



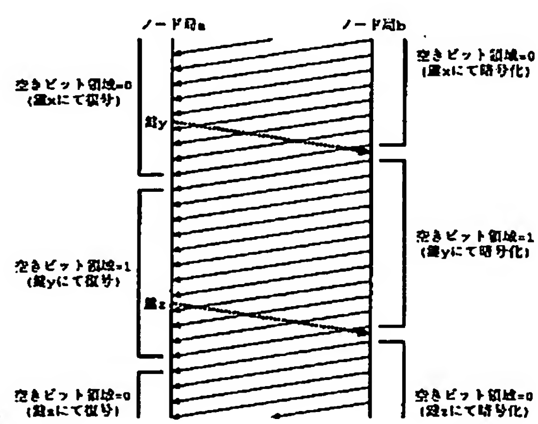
【図１７】



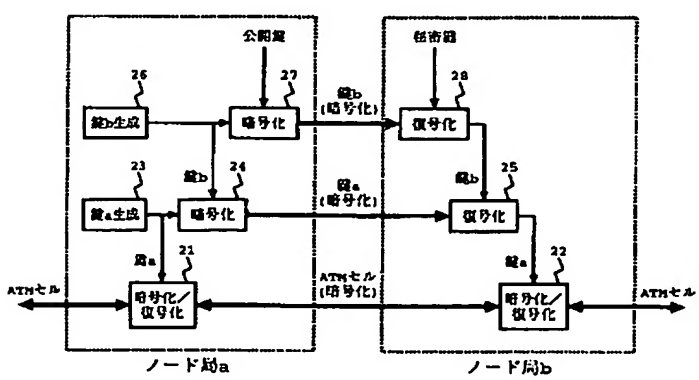
【図２３】



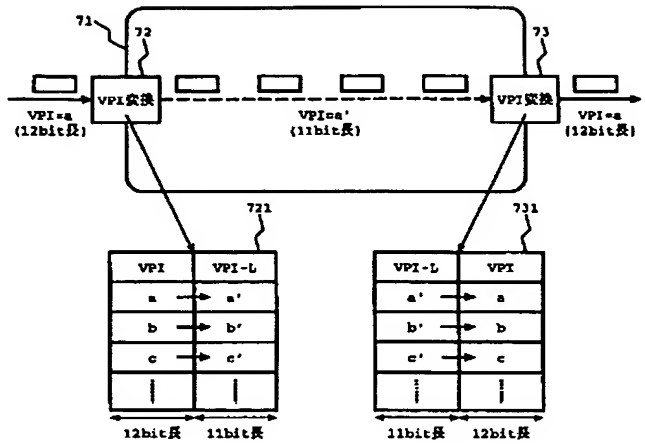
【図２４】



【図１９】



【図２１】



フロントページの続き

(72)発明者　角田　啓治
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

Ｆターム(参考)　5J104 AA01 AA16 AA34 EA17 EA19
JA13 JA28 JA31 NA02 PA01
5K030 GA15 HA10 HB11 HB29 HC14
JL01 JT09 LD19
9A001 CC02 CC05 CC08 EE03 EE04
HH15 JJ12 KK56 LL03